

REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed June 28, 2005. Reconsideration and allowance of the application and pending claims are respectfully requested.

I. Claim Rejections - 35 U.S.C. § 102(e)

Claims 1-30 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Strahm et al. ("Strahm," U.S. Pub. No. 2002/0104020). Applicant respectfully traverses this rejection.

It is axiomatic that "[a]nticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W. L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 USPQ 303, 313 (Fed. Cir. 1983). Therefore, every claimed feature of the claimed invention must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. § 102(e).

In the present case, not every feature of the claimed invention is represented in the Strahm reference. Applicant discusses the Strahm reference and Applicant's claims in the following.

A. The Strahm Reference

Strahm discloses a system for processing Internet protocol security (IPSec) traffic. Strahm, Application Title. As is described by Strahm, packets sent from a source (e.g., CE 202) arrive at a CFE 202, which attempts to classify the packet. Strahm, paragraph 0029. As is described by Strahm, the CFE 202 classifies the packet by accessing the packet's contents. Strahm, paragraph 0029.

Once the packet is classified, the CFE 202 forwards (i.e., routes) the packet to any one of multiple DFEs 204. Strahm, paragraph 0030. As is described by Strahm, the decision as to which DFE to route the packet to is unimportant. Specifically, Strahm states:

The CFE 202 can use any selection technique to choose which DFE 204a-204c receives the packet 210. For example, the CFE 202 could implement a load balancing technique that distributes packets to the DFEs 204a-204c based on resource availability of the DFEs 204a-204c and/or the servers 214a-214c associated with the DFEs 204a-204c. In another example, the CFE 202 could implement a fixed scheme that distributed packets to the DFEs 204a-204c based on a fixed rotating order or based on a round robin scheme.

[Strahm, paragraph 0030]

Although Strahm states that the packet may include a security association (SA), Strahm says *nothing* about deciding where to route a packet to based upon a security association of the packet.

B. Applicant's Claims

1. Claims 1-14

Applicant's claim 1 provides as follows (emphasis added):

1. An apparatus for performing network routing, the apparatus comprising:

authentication logic configured to receive packets sent from a source agent to an endpoint of a tunnel and to determine whether a security association of a packet received corresponds to said source

agent, the tunnel being configured by said source agent in accordance with a network protocol;

decision logic configured to make a routing decision for each authenticated packet that is constrained based on the security association of the authenticated packet; and

routing logic configured to select a routing destination for each authenticated packet and to route the authenticated packet to the selected routing destination, the routing destination selection being based at least partially on said routing decision.

In the Office Action, it is argued that Strahm teaches decision logic configured to make a routing decision for each authenticated packet that is constrained based on the security association of the authenticated packet. This argument is not supported by Strahm's disclosure.

Strahm describes his disclosed method for processing packets in detail in paragraphs 0029 to 0036. As is explained in those paragraphs, and as is summarized above, a packet 210 arrives at the classifying forwarding element (CFE) that has the responsibility of "classifying" the packet. Strahm, paragraph 0029. Once the packet is received, flow depends upon whether the packet is encrypted.

If the received packet is not encrypted (i.e., the packet is "in the clear"), the CFE accesses the packet's contents and "classifies" the packet based upon the information contained in those contents. Strahm, paragraph 0029. After the classifying has been completed, the CFE forwards the classified packet to one of several decrypting forwarding elements (DFEs). Strahm, paragraph 0030. Regardless, the CFE does not make a routing decision based on a "security association". Instead, routing from the CFE is much more arbitrary (see excerpt from paragraph 0030 reproduced above).

As a further point, Applicant notes that it cannot simply be presumed that Strahm uses the security association to make the routing decision. Indeed, if any presumption is to be made, the *opposite* should be presumed. Specifically, as is described in Applicant's original disclosure, the security association is normally *not* used to make a routing decision according to IPSec protocol. As is stated in that disclosure:

. . . each IPSec packet will include a destination IP address, an ESP header, and a payload. The payload includes, among other information, an internal destination address and data, both of which may be encrypted. As stated above, if the payload packet is successfully authenticated at the destination endpoint, the decrypted internal destination address is normally used by the endpoint device to determine the destination to which the decrypted packet is to be routed within the private network.

[Applicant's specification, page 15, lines 14-19]

As is apparent from the above, then, the typical practice in IPSec protocol is to *ignore* the address of security association and instead consult the destination address contained in the packet payload to determine where to send the packet. Regardless, it is clear that Strahm's system does not use any address in a security association to make a routing decision. Indeed, Strahm is not concerned about routing to particular destinations. More important to Strahm are things like "load balancing" and the like (see Strahm, paragraph 0030).

In view of the above, it is clear that Strahm's CFE does not comprise "decision logic configured to make a routing decision for each authenticated packet that is constrained based on the security association of the authenticated packet", as is

required by claim 1. Applicant's claims 1-14 are allowable over Strahm for at least this reason.

In the outstanding Office Action, the Examiner argues that Strahm discloses that the CFE "classifies" the traffic to make the routing decision. This is not true. Although Strahm does disclose classifying packets that are received, the classification is *not* used to determine where the packet is routed to. Again, routing is merely based upon load balancing concerns or which DFE 204 is the "next" one that should receive a packet in a "round robin" scheme (see Strahm, paragraph 0030). Therefore, "classification" is independent of the routing decision. Indeed, Strahm even speaks of routing *unclassified* packets in paragraph 0039. There, Strahm states:

In another example, the CFE 202 may have forwarded a copy of the packet 210 to the DFE 204a in which case the CFE 202 still has the unclassified packet 210. The packet 210 may not need classification by the CFE 202 for a variety of reasons."

[Strahm, paragraph 0030]

Therefore, Strahm's routing is not dependent upon the particular classification that is performed.

2. Claims 15-23

Applicant's claim 15 provides as follows (emphasis added):

15. A method for performing network routing, the method comprising:

authenticating received packets sent from a source agent to an endpoint of a tunnel by determining whether a security association of a received packet corresponds to the source agent that sent the packet,

the tunnel being configured by said source agent in accordance with a network protocol;

making a routing decision for an authenticated packet, the routing decision being constrained based on the security association of the authenticated packet;

selecting a routing destination for a packet based at least partially on the routing decision; and

routing the authenticated packet to the selected routing destination.

As is described above in relation to claim 1, Strahm's CFE does not, as is suggested in the Office Action, control routing based on a security association. It logically follows that Strahm's CFE does not make "a routing decision for an authenticated packet, the routing decision being constrained based on the security association of the authenticated packet" or "selecting a routing destination for a packet based at least partially on the routing decision". Claims 15-23 are allowable over Strahm for at least this reason.

3. Claims 24-25

Applicant's claim 24 provides as follows (emphasis added):

24. A computer program for performing network routing in accordance with a private network security technique, the computer program being embodied on a computer readable medium, the computer program comprising:

a first code segment, the first code segment authenticating received packets sent from a source agent to a tunnel endpoint to determine whether a security association of a received packet

corresponds to the source agent that sent the packet, the tunnel being configured by said source in accordance with a network protocol;

a second code segment, *the second code segment making a routing decision for an authenticated packet, the routing decision being constrained based on the security association of the authenticated*; and

a third code segment, *the third code segment selecting a routing destination for the authenticated packet based at least partially on the routing decision made by the second code segment*.

As is described above in relation to claim 1, Strahm's CFE does not, as is suggested in the Office Action, control routing based on a security association. It logically follows that Strahm's CFE does not include a code segment that makes "a routing decision for an authenticated packet, the routing decision being constrained based on the security association of the authenticated" or a code segment that selects "a routing destination for the authenticated packet based at least partially on the routing decision made by the second code segment". Claims 24 and 25 are allowable over Strahm for at least this reason.

4. Claims 26-30

Applicant's claim 26 provides as follows (emphasis added):

26. A method for routing a packet, comprising:
receiving a packet at a tunnel endpoint;
authenticating the packet;
preserving a security association of the packet as an authentication ID;

making a routing determination for routing contents of the packet by looking up the authentication ID in a table to determine a destination IP address to which the packet is to be routed.

Regarding claim 26, the Office Action states that Strahm discloses making a routing decision by looking up the authentication ID in a table to determine a destination IP address to which the packet is to be routed and cites paragraph 0010, lines 1-7. Applicant disagrees. That portion of the Strahm disclosure provides as follows:

SPIs are identifiers, each uniquely associated with a security association (SA) relative to a security protocol. The source and the destination of packets transferred with IPsec need to establish an SA. An SA is a set of agreements between a packet's source and destination that determine the protocols used in transmitting the packet between the source and the destination.

[Strahm, paragraph 0010, lines 1-7]

As is apparent from the above excerpt, Strahm does *not* describe making a routing decision by looking up the authentication ID in a table to determine a destination IP address. Indeed, Strahm says *nothing whatsoever* about a “table” or looking up an address in such a table. Given that Strahm does not teach this aspect of claim 26, claims 26-30 are allowable over Strahm.

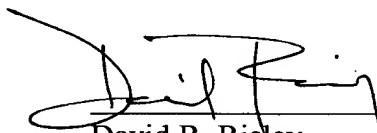
C. Conclusion

Due to the shortcomings of the Strahm reference described in the foregoing, Applicant respectfully asserts that Strahm does not anticipate Applicant's claims. Therefore, Applicant respectfully requests that the rejection of these claims be withdrawn.

CONCLUSION

Applicant respectfully submits that Applicant's pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

Respectfully submitted,


David R. Risley
Registration No. 39,345

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postage prepaid, in an envelope addressed to: Assistant Commissioner for Patents, Alexandria, Virginia 22313-1450, on

9-27-05
Mary Meepa
Signature